

[ORAL ARGUMENT NOT YET SCHEDULED]
No. 14-5013

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff-Appellee,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY,

Defendant-Appellant.

On Appeal from the United States District Court for the District of Columbia

BRIEF FOR APPELLANT

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

SHARON SWINGLE
ADAM C. JED
(202) 514-8280
Attorneys, Appellate Staff
Civil Division, Room 7240
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, DC 20530

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties and Amici

The plaintiff-appellee is the Electronic Privacy Information Center. The defendant-appellant is the United States Department of Homeland Security.

B. Rulings Under Review

The defendant-appellant seeks review of the November 12, 2013 judgment and decision, issued by the Honorable James E. Boasberg, United States District Court for the District of Columbia, in Case No. 13-cv-260, ECF Nos. 18, 19. The district court's order and opinion are reproduced in the Joint Appendix at JA41 and JA42 respectively. No citation is yet available in the Federal Supplement. The district court's opinion can be found at 2013 WL 5976973.

C. Related Cases

This case has not previously been before this or any other court. We are not aware of any related cases.

TABLE OF CONTENTS

	<u>Page</u>
CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES	
GLOSSARY	
STATEMENT OF JURISDICTION	1
STATEMENT OF THE ISSUES	2
PERTINENT STATUTES AND REGULATIONS.....	2
STATEMENT OF THE CASE	2
A. Statutory Background	2
B. Factual Background and Prior Proceedings.....	3
SUMMARY OF ARGUMENT	6
STANDARD OF REVIEW.....	9
ARGUMENT	9
The Department of Homeland Security's Standard Operating Procedure 303 is Exempt From Disclosure Under FOIA.....	9
A. The Department of Homeland Security Properly Withheld SOP 303 Under FOIA Exemption 7(F)	10
B. The Department of Homeland Security Properly Withheld SOP 303 Under FOIA Exemption 7(E).....	21
CONCLUSION	28
CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32(a)	
CERTIFICATE OF SERVICE	

TABLE OF AUTHORITIES

Cases:	<u>Page</u>
<i>ACLU v. Dep't of Defense</i> , 543 F.3d 59 (2d Cir. 2008), <i>vacated on other grounds</i> , 558 U.S. 1042 (2009)	6
<i>Ali v. Fed. Bureau of Prisons</i> , 552 U.S. 214 (2008)	11, 12
<i>Baldrige v. Shapiro</i> , 455 U.S. 345 (1982)	2
<i>Boyle v. United States</i> , 556 U.S. 938 (2009)	12, 14
<i>CLA v. Sims</i> , 471 U.S. 159 (1985)	12
<i>FBI v. Abramson</i> , 456 U.S. 615 (1982)	3, 17
<i>John Doe Agency v. John Doe Corp.</i> , 493 U.S. 146, 152 (1989)	2, 3
<i>Kasten v. Saint-Gobain Performance Plastics Corp.</i> , 131 S. Ct. 1325 (2011)	12
<i>Kissinger v. Reporters Comm. for Freedom of the Press</i> , 445 U.S. 136 (1980)	17
<i>LaRouche v. Webster</i> , No. 75-cv-6010, 1984 WL 1061 (S.D.N.Y. Oct. 23, 1984)	17, 19
<i>Living Rivers, Inc. v. U.S. Bureau of Reclamation</i> , 272 F. Supp. 2d 1313 (D. Utah 2003)	20

* Authorities upon which we chiefly rely are marked with asterisks.

<i>Los Angeles Times Commc'ns, LLC v. Dep't of the Army</i> , 442 F. Supp. 2d 880 (C.D. Cal. 2006)	20
<i>Massachusetts v. EPA</i> , 549 U.S. 497 (2007)	12
<i>Milner v. Dep't of the Navy</i> , 131 S. Ct. 1259 (2011)	5, 10
<i>Norfolk S. Ry. v. James N. Kirby, Pty Ltd.</i> , 543 U.S. 14 (2004)	12
<i>Peter S. Herrick's Customs & Int'l Trade Newsletter v. U.S. Customs & Border Prot.</i> , No. 04-377, 2006 WL 1826185 (D.D.C. June 30, 2006)	19
<i>*Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int'l Bound. & Water Comm'n, U.S.-Mexico</i> , 740 F.3d 195 (D.C. Cir. 2014)	9, 10, 11, 19, 27
<i>Salinas v. United States</i> , 552 U.S. 52 (1997)	12
<i>Shaver v. Bell</i> , 433 F. Supp. 438 (N.D. Ga. 1977)	22
<i>Sladek v. Bensinger</i> , 605 F.2d 899 (5th Cir. 1979)	22
<i>Tax Analysts v. IRS</i> , 294 F.3d 71 (D.C. Cir. 2002)	23
<i>United States v. Gonzales</i> , 520 U.S. 1 (1997)	12
<i>U.S. Dep't of State v. Washington Post Co.</i> , 456 U.S. 595 (1982)	17

Statutes:

5 U.S.C. § 552.....	2
5 U.S.C. § 552(a)(4)(A)(vii)	1
5 U.S.C. § 552(a)(4)(B)	1
5 U.S.C. § 552(a)(6)(C)(i)	1
5 U.S.C. § 552(b)(7)	3, 5
5 U.S.C. § 552(b)(7)(A)-(C)	13
*5 U.S.C. § 552(b)(7)(E).....	2, 3, 7, 8, 13, 21, 23, 25, 26
*5 U.S.C. § 552(b)(7)(E) (1982)	8, 21, 26
*5 U.S.C. § 552(b)(7)(F)	2, 3, 6, 10, 11, 21
5 U.S.C. § 552a(a)(6).....	12
5 U.S.C. § 552a(j)(2)(B)	12
5 U.S.C. § 552a(l)(2).....	12
5 U.S.C. § 552a(l)(3).....	12
28 U.S.C. § 1291	1
28 U.S.C. § 1331	1
Freedom of Information Reform Act of 1986, Pub. L. No. 99-570, Tit. I, Subtit. N, § 1802(a), 100 Stat. 3207-48	15, 16

Rules:

Fed. R. App. P. 4(a)(1)(B).....	1
Fed. R. App. P. 26(a)(1)(C).....	1

Legislative Materials:

130 Cong. Rec. (1984):

p. 3502 15

p. 3521 15

131 Cong. Rec. (1985):

p. 248 18

p. 253 18

132 Cong. Rec. (1986):

p. 26,111 15, 16

p. 26,473 16

p. 26,770 15, 16

p. 27,189 13, 15, 16

p. 27,208 16

p. 27,251-27,252 16

p. 29,616 18

p. 29,619 13, 15, 16

p. 29,652 16

p. 31,423-31,424 13, 15, 16, 18

p. 31,424 14

1 <i>Freedom of Information Act: Hearings Before the Subcomm. on the Constitution of the Senate Comm. on the Judiciary</i> , 97th Cong., 1st Sess. (1981)	14, 15
H.R. Rep. No. 89-1497 (1966)	2
*S. Rep. No. 98-221 (1983)	8, 13, 15, 23, 24, 25

Other Authorities:

U.S. Dep't of Justice, <i>Attorney General's Memorandum on the 1986 Amendments to the Freedom of Information Act</i> (1987)	16, 24
---	--------

GLOSSARY

DHS Department of Homeland Security

EPIC Electronic Privacy Information Center

FOIA Freedom of Information Act

JA Joint Appendix

SOP 303 Department of Homeland Security Standard Operating Procedure 303

[ORAL ARGUMENT NOT YET SCHEDULED]
No. 14-5013

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff-Appellee,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY,

Defendant-Appellant.

On Appeal from the United States District Court for the District of Columbia

BRIEF FOR APPELLANT

STATEMENT OF JURISDICTION

The plaintiff invoked the jurisdiction of the district court under 5 U.S.C. §§ 552(a)(4)(A)(vii), (a)(4)(B), (a)(6)(C)(i), and 28 U.S.C. § 1331. JA 2. The district court entered final judgment for the plaintiff on November 12, 2013. JA 41; see also JA 42-57 (opinion). The government filed a timely notice of appeal on January 13, 2014. JA 58; see Fed. R. App. P. 4(a)(1)(B); see also Fed. R. App. P. 26(a)(1)(C). This Court has appellate jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

Whether the Department of Homeland Security's standard operating procedure for coordinating the shutdown and restoration of wireless networks during critical emergencies, such as the threatened use of wireless-activated explosive devices, is exempt under Exemptions 7(E) or 7(F) of the Freedom of Information Act, 5 U.S.C. § 552(b)(7)(E) and (F).

PERTINENT STATUTES AND REGULATIONS

Pertinent provisions are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

A. Statutory Background

The Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, strikes a "workable balance between the right of the public to know and the need of the Government to keep information in confidence." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989) (quoting H.R. Rep. No. 89-1497, at 6 (1966)). Thus, the Act generally "provide[s] for open disclosure of public information" but "recognizes" through nine statutory exemptions that certain "disclosure is not always in the public interest." *Baldrige v. Shapiro*, 455 U.S. 345, 352 (1982).

"Congress realized that legitimate governmental and private interests could be harmed by release of certain types of information, and therefore provided the specific exemptions under which disclosure could be refused." *John Doe Agency*, 493 U.S. at 152 (internal quotation marks omitted). These exemptions "are intended to have

meaningful reach and application.” *Ibid.* Courts “tak[e] a practical approach” in interpreting the FOIA exemptions. *Id.* at 157; see also *FBI v. Abramson*, 456 U.S. 615, 630-631 (1982).

FOIA Exemption 7 protects from disclosure various “records or information compiled for law enforcement purposes.” 5 U.S.C. § 552(b)(7). As relevant here, FOIA Exemption 7 shields such records that “could reasonably be expected to endanger the life or physical safety of any individual,” 5 U.S.C. § 552(b)(7)(F), or that “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law,” 5 U.S.C. § 552(b)(7)(E).

B. Factual Background and Prior Proceedings

1. The Department of Homeland Security’s (DHS) Standard Operating Procedure 303 (SOP 303) is a procedure for determining if and when wireless networks should be shut down and restored “during critical emergencies such as the threat of radio-activated improvised explosive devices,” and for executing voluntary shutdowns and restorations. JA 16-19. SOP 303 was created after the 2005 bombings of the London transportation system to address shortcomings in the United States’ ability to address such threats. JA 16; see also JA 39-40. SOP 303 “establishes a protocol for verifying that circumstances exist that would justify shutting down wireless networks,” and steps for taking into account the detrimental

effects of shutting down wireless networks, such as “the inability of first-responders and the public to use wireless phones for calls, including 911 calls.” JA 18. SOP 303 also establishes a “step-by-step process for the orderly shut-down of wireless networks,” such as authentication protocols to prove that a requester is authorized to initiate a shutoff. *Ibid.* It includes similar procedures and authentication protocols for restoring communications. *Ibid.*

2. Plaintiff, the Electronic Privacy Information Center (“EPIC”), filed a Freedom of Information Act request with DHS seeking the full text of SOP 303, the full set of questions for deciding whether a shutdown is necessary, and any related protocols and guidelines. JA 12; see JA 27.

After EPIC brought suit, and following an administrative appeal, DHS identified one responsive document, SOP 303, which DHS released in substantially redacted form. JA12-19; see also JA38 (*Vaughn* Index). DHS withheld much of the document under Exemptions 7(E) and 7(F). See JA 17-19, 38.¹ DHS concluded that “[m]aking SOP 303 public would enable bad actors to circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices by providing information about when shutdown procedures are used and how a shutdown is executed.” JA 18. It would also “enable bad actors to insert

¹ Pursuant to FOIA Exemptions 6 and 7(C), which concern invasions of personal privacy, DHS also withheld the names, direct-dial telephone numbers, and email addresses for state homeland security officials JA 17-18. Those redactions are not at issue here.

themselves into the process of shutting down or reactivating wireless networks by appropriating verification methods and then impersonating officials designated for involvement in the verification process.” JA 19. Using SOP 303, bad actors could “disable the protocol so that they could freely use wireless networks to activate the improvised explosive devices.” *Ibid.*

3. The district court granted summary judgment for EPIC, rejecting DHS’s Exemption 7 claims and ordering that DHS turn over SOP 303 with only redactions for personal privacy. JA 57.² The court agreed with the government that SOP 303 was “compiled for law enforcement purposes,” 5 U.S.C. § 552(b)(7). JA 46-49, 51 (citing, *inter alia*, *Milner v. Dep’t of the Navy*, 131 S. Ct. 1259, 1272 (2011) (Alito, J., concurring) (“[S]teps by law enforcement officers to prevent terrorism surely fulfill ‘law enforcement purposes.’”). The court held, however, that SOP 303 does not satisfy the additional requirements of Exemptions 7(E) and 7(F). JA 48-56.

The court held that Exemption 7(E)’s protection for records that “would disclose techniques and procedures for law enforcement investigations or prosecutions” does not apply. JA 47-50. The court concluded that Exemption 7(E) encompasses only “acts by law enforcement after or during the commission of a crime, not crime-prevention techniques.” JA 48-49. The court rejected DHS’s arguments that, even if Exemption 7(E) is construed in this manner, it applies here

² The district court stayed its order pending the government’s appeal. See JA 41, 57; Minute Order (Nov. 22, 2013).

because SOP 303 helps to preserve evidence and track suspects. JA50. The court reasoned that, because SOP 303 is primarily a protocol for shutting down wireless networks to deter the triggering of explosives, an “ordinary speaker” would not “describe SOP 303 . . . as an evidence-gathering technique.” *Ibid.*

The court also held inapplicable Exemption 7(F)’s protection for records where disclosure “could reasonably be expected to endanger the life or physical safety of any individual,” 5 U.S.C. § 552(b)(7)(F). JA 51-56. The court rejected DHS’s argument that release of SOP 303 would enable bad actors to blunt the usefulness of the protocol and to detonate bombs remotely. JA 51. The court concluded that Exemption 7(F)’s requirement of endangering “any individual” applies only if the agency “identif[ies] the individuals at risk with some degree of specificity.” JA 51-52 (citing *ACLU v. Dep’t of Defense*, 543 F.3d 59, 66-72 (2d Cir. 2008), *vacated on other grounds*, 558 U.S. 1042 (2009)). The court concluded that it is not sufficiently specific to identify individuals “within the blast radius of a remotely detonated bomb.” JA 54.

SUMMARY OF ARGUMENT

A. DHS properly withheld SOP 303 under FOIA Exemption 7(F), which shields from disclosure records that “could reasonably be expected to endanger the life or physical safety of any individual,” 5 U.S.C. § 552(b)(7)(F). DHS explained that “[m]aking SOP 303 public would enable bad actors to circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices” and “to insert themselves into the process of shutting down or reactivating

wireless networks by appropriating verification methods and then impersonating officials designated for involvement in the verification process.” JA 18-19. Using SOP 303, bad actors “could freely use wireless networks to activate the improvised explosive devices.” JA 19.

The district court held that Exemption 7(F) applies only if the agency “identif[ies] the individuals at risk with some degree of specificity.” JA 51-52. But the broad language of Exemption 7(F) does not include any such limitation. And there is no compelling reason to imply such an atextual requirement, particularly where weighty interests—“life or physical safety”—are at stake. The district court’s interpretation would lead to the anomalous result that an agency may withhold a document if disclosure poses a danger to a small group of specifically identifiable people but must produce a document if disclosure poses a danger to many or most people. In any event, the government identified the individuals most likely to be at risk with the requisite degree of specificity.

B. DHS also properly withheld SOP 303 under FOIA Exemption 7(E), which protects against disclosure of “techniques and procedures for law enforcement investigations or prosecutions,” as well as “guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law,” 5 U.S.C. § 552(b)(7)(E). The district court held that because an “ordinary speaker” would not “describe SOP 303 . . . as an evidence-gathering technique,” Exemption 7(E) is therefore inapplicable. JA 50. But the

court's reasoning is at odds with the text and history of Exemption 7(E). The pre-1986 version of Exemption 7(E) required that production would “disclose *investigative* techniques and procedures,” 5 U.S.C. § 552(b)(7)(E) (1982) (emphasis added), *i.e.*, specific types of “techniques and procedures” that are “investigative” in nature. But in 1986, Congress deleted the word “investigative,” and added the phrase “*for* law enforcement investigations or prosecutions.” This change “ma[d]e clear that ‘techniques and procedures for law enforcement investigations and prosecutions’ can be protected, regardless of whether they are ‘investigative’ or non-investigative.” S. Rep. No. 98-221, at 24 (1983) (“Senate Report”).

SOP 303 involves techniques and procedures for carrying out law enforcement investigations. SOP 303 contains procedures that apply only when there is a serious threat, which undoubtedly will trigger a law enforcement investigation. Choosing whether, when, and where to shut down a cellular network is a logical component of an ongoing investigation triggered by the threat. As such, the procedures in SOP 303 are procedures “*for* law enforcement investigations,” 5 U.S.C. § 552(b)(7)(E) (emphasis added), even if the procedures may not themselves be deemed “investigative” in nature. See Senate Report 24 (procedures themselves need not be “investigative” to be covered by Exemption 7(E)). Moreover, SOP 303 sets out procedures that directly support such investigations. SOP 303's procedures balance the aim of “preventing and/or mitigating explosions” with the deleterious effects of a wireless shutdown on “first-responders” and on “the public[’s] use [of] wireless

phones for calls, including 911 calls.” JA 18. Preventing bombs from being detonated protects first responders who are investigating the events, witnesses who can offer helpful clues, and valuable physical evidence such as undetonated bombs. Ensuring that first responders such as police bomb squads and arson units can quickly and effectively deploy, and that the public can make wireless calls, including 911 calls, also helps to obtain valuable information.

STANDARD OF REVIEW

The district court’s grant of summary judgment is reviewed de novo. *Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int’l Boundary & Water Comm’n, U.S.-Mexico*, 740 F.3d 195, 200 (D.C. Cir. 2014).

ARGUMENT

The Department of Homeland Security’s Standard Operating Procedure 303 Is Exempt From Disclosure Under FOIA

The Department of Homeland Security’s Standard Operating Procedure 303 is a protocol for coordinating among government officials and wireless service providers to determine if and when wireless networks should be shut down and restored “during critical emergencies such as the threat of radio-activated improvised explosive devices.” JA 16-19. SOP 303 establishes a protocol for determining which threats warrant a wireless shutdown and for taking into the account the effects of a shutdown on first responders and the public’s use of wireless phones to make calls, such as 911

calls. JA 18. It also establishes a protocol for securely shutting down and restoring wireless communications. *Ibid.*

The district court correctly held that SOP 303 meets the threshold requirement of FOIA Exemption 7 of being “records or information compiled for law enforcement purposes.” JA 46-49, 51. SOP 303 was created after the 2005 bombings of the London transportation system to address shortcomings in the United States’ ability to address and respond to such threats. JA 16; see also JA 39-40. This is plainly a “law enforcement purpose.” See *Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int’l Bound. & Water Comm’n, U.S.-Mexico (“PEER”)*, 740 F.3d 195, 203-204 (D.C. Cir. 2014) (holding that this includes “proactive steps designed to prevent criminal activity and to maintain security” and “surely” includes “steps by law enforcement officers to prevent terrorism”) (quoting *Milner v. Dep’t of the Navy*, 131 S. Ct. 1259, 1272 (2011) (Alito, J., concurring)). The district court erred, however, in concluding that SOP 303 is not covered by either Exemption 7(F) or Exemption 7(E).

A. The Department of Homeland Security Properly Withheld SOP 303 Under FOIA Exemption 7(F).

1. FOIA Exemption 7(F) shields from disclosure records that “could reasonably be expected to endanger the life or physical safety of any individual,” 5 U.S.C. § 552(b)(7)(F). As this Court has observed, “[t]hat language is very broad.” *PEER*, 740 F.3d at 205. The government “need only demonstrate that it reasonably estimated that sensitive information could be misused for nefarious ends.” *Id.* at 206.

When a document “relat[es] to critical infrastructure, such as blueprints, maps, and emergency plans,” “it is not difficult to show that disclosure may endanger the life or physical safety of any individual.” *Id.* at 205-206 (emphasizing that courts “have consistently deferred to executive affidavits predicting harm to the national security”) (internal quotation marks omitted).

SOP 303 easily meets this requirement. DHS explained that “[m]aking SOP 303 public would enable bad actors to circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices.” JA 18. Bad actors could “insert themselves into the process of shutting down or reactivating wireless networks by appropriating verification methods and then impersonating officials designated for involvement in the verification process.” JA 19. Once the protocol was disabled, bad actors “could freely use wireless networks to activate the improvised explosive devices.” *Ibid.*

2. The district court erred in construing Exemption 7(F) to apply only where producing records or information could endanger the life or physical safety of specifically identified individuals. JA 51-52.

Exemption 7(F) shields from disclosure records that “could reasonably be expected to endanger the life or physical safety of *any* individual.” 5 U.S.C. § 552(b)(7)(F) (emphasis added). That “language is very broad.” *PEER*, 740 F.3d at 205. “[R]ead naturally, the word ‘any’ has an expansive meaning, that is, ‘one or some indiscriminately of whatever kind.’” *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 219

(2008) (quoting *United States v. Gonzales*, 520 U.S. 1, 5 (1997)); see *Norfolk S. Ry. v. James N. Kirby, Pty Ltd.*, 543 U.S. 14, 31 (2004); see also *Kasten v. Saint-Gobain Performance Plastics Corp.*, 131 S. Ct. 1325, 1332 (2011) (“‘any complaint’ suggests a broad interpretation”); *Boyle v. United States*, 556 U.S. 938, 944 (2009) (“The term ‘any’ [in a definitional provision] ensures that the definition has a wide reach.”); *Massachusetts v. EPA*, 549 U.S. 497, 528-529 (2007) (use of the word “any” underscores intent to have broad scope); *Salinas v. United States*, 522 U.S. 52, 56-57 (1997) (“any” suggests that the scope is “expansive” and “unqualified”). In the absence of “language limiting the breadth of that word,” the term “any” should be given this normal, expansive meaning. *Gonzales*, 520 U.S. at 5 (citing cases); see *Ali*, 552 U.S. at 220 n.4.

The district court construed the reference to “any individual” to mean “any *specifically identified* individual.” Although Congress easily could have imposed that limitation, it did not do so. In contrast, FOIA’s companion statute, the Privacy Act, affords special treatment to certain law enforcement records associated with an “identifiable individual,” 5 U.S.C. § 552a(j)(2)(B); see also 5 U.S.C. § 552a(a)(6), (j)(2) and (3) (other requirements pertaining to “an identifiable individual”); cf. *CLA v. Sims*, 471 U.S. 159, 169 n.13 (1985) (relying on Privacy Act to construe FOIA). But Congress did not similarly limit the scope of FOIA Exemption 7(F) to harms faced only by an “identifiable individual”—or, as the district court put it, an “individual” “identif[ied] . . . with reasonable specificity.” JA 51-52.

Exemption 7(F) guards particularly weighty interests in “life or physical safety.” The district court’s interpretation would lead to the anomalous result that an agency could withhold a document if disclosure posed a danger to a small group of people but would be required to produce the document if disclosure posed a danger to many or most people. Given that other provisions in Exemption 7 permit the withholding of records to advance interests such as protecting personal privacy, noninterference with civil enforcement proceedings, ensuring impartial adjudications, and preventing circumvention of the law, see 5 U.S.C. § 552(b)(7)(A)-(C) and (E), it is difficult to believe that Congress did not intend to allow the withholding of information when disclosure could lead to such widespread deaths that the victims could not easily be identified in advance.

Indeed, when Congress amended Exemption 7(F) in 1986 to expand its coverage from danger to “law enforcement personnel” to danger to “any individual,” Congress also changed the required degree of risk from “would endanger” to “could reasonably be expected to endanger.” See S. Rep. No. 98-221, at 23-24 (1983) (“Senate Report”) (noting the “lack of certainty in attempting to predict harm”)³; see

³ Although Senate Report No. 221 accompanied S. 774 in the 98th Congress, the legislative history from the 99th Congress shows that the 1986 amendments to Exemption 7 adopted text “identical” to that in S. 774 and that Senate Report No. 221 thus explains the “meaning and intended effect of the [1986] amendments.” 132 Cong. Rec. 27,189 (1986) (Sen. Leahy); *id.* at 31,423-31,424 (Sen. Hatch) (revisions to Exemption 7 “derive precisely” from S. 774); *id.* at 29,619 (Rep. Kindness)

Continued on next page.

also 132 Cong. Rec. 31,424 (1986) (statement of Sen. Hatch, principal sponsor of amendments, explaining that they were intended to “ease considerably” an “agency’s burden in invoking” Exemption 7’s protections). Given this history, it would make little sense to construe the change as heightening the necessary showing by the government.

The district court observed that, when Congress was considering amending Exemption 7(F), the Deputy Attorney General and one member of Congress expressed concern that the then-existing version of Exemption 7(F), which covered danger to “law enforcement personnel,” did not address danger to other persons, such as victims, witnesses, informants, and families of law enforcement personnel. JA 52-53. And the court stated that the Deputy Attorney General and another member of Congress described the amendment as “modest” and a “slight expan[sion].” JA 53. The legislative history fails to support the district court’s limiting construction. The 1986 amendment derives from an earlier proposal by the Department of Justice to replace the term “law enforcement personnel” with the term “any natural person.” 1 *Freedom of Information Act: Hearings Before the Subcomm. on the Constitution of the Senate Comm. on the Judiciary*, 97th Cong., 1st Sess. 178, 182 (1981) (“1981 Hearings”). The Department of Justice explained that there was “no reason” for protecting “law enforcement personnel to the exclusion of all others,” and that

(reproducing S. Rep. No. 211 in pertinent part and explaining that the Senate Report on S. 774 reflects the “meaning and intended effect of the [House] amendments”).

records should be exempt whenever “the life or personal safety of any person would be endangered by their release.” *Id.* at 189, 200. As then-Professor Scalia testified, Exemption 7(F)’s coverage only of danger to law enforcement personnel was “inadequa[te]” and “almost irrational[]” and did not adequately protect the serious interests at stake. *Id.* at 959-960; see also *id.* at 870, 917 (testimony of others that Exemption 7(F) was “too narrow and should be expanded to protect the life and physical safety o[f] ‘any natural person’”); *id.* at 518 (testimony of others observing that, if people’s “privacy is worthy of protection, so are their lives”).

Several bills incorporating the suggested revision were introduced in the 97th Congress, but none was enacted. Similar bills were then introduced in the 98th and 99th Congress, one of which was subsequently enacted into law. See Freedom of Information Reform Act of 1986, Pub. L. No. 99-570, Tit. I, Subtit. N, § 1802(a), 100 Stat. 3207-48. The legislative history shows that the enacted bill was understood to be identical in effect to the earlier bills. See Senate Report 3-6, 23; 130 Cong. Rec. 3502 (1984); 132 Cong. Rec. 26,111, 26,770, 27,189, 29,619, 31,423-31,424 (1986).⁴

⁴ Several bills in the 97th Congress, including one introduced by Senator Hatch (S. 1730), incorporated the Justice Department’s recommendation to extend Exemption 7(F)’s protections to “any natural person.” 1981 *Hearings* 8, 30, 50, 67. In the 98th Congress, Senator Hatch introduced S. 774 based on his bill in the previous Congress, proposing again to extend Exemption 7(F)’s protections to “any natural person.” Senate Report 3-6 (emphasis omitted) (explaining that S. 774 “is virtually identical to S. 1730” and recounting S. 1730’s history in the 97th Congress). Senator Hatch invoked “the [testimony] of Professor Scalia.” 130 Cong. Rec. 3502 (1984). S. 774 passed the Senate, 130 Cong. Rec. 3521 (1984), but it did not pass the House of

Continued on next page.

Shortly after the 1986 amendments, the Attorney General issued guidance to federal agencies explaining the amendments' scope. See U.S. Dep't of Justice, *Attorney General's Memorandum on the 1986 Amendments to the Freedom of Information Act* (1987) ("*Attorney General's Memorandum*"). The Attorney General explained that Congress's expansion of Exemption 7(F) to "encompass 'any individual' is obviously designed to ensure that no law enforcement information that could endanger *anyone* if disclosed . . . should ever be required to be released" under FOIA. *Id.* at 18 (emphasis added). In light of that "clear authority" to withhold documents "endangering any person," the Attorney General instructed that "agencies should take pains to ensure that they withhold any information that, if disclosed under the FOIA, could reasonably be

Representatives before the end of the 98th Congress. The portion of S. 774 amending FOIA Exemption 7 was then reintroduced in the 99th Congress as part of a Senate bill (S. 2878), which the Senate adopted and passed as an amendment to the Anti-Drug Abuse Act of 1986 (H.R. 5484). See 132 Cong. Rec. 26,111 (1986) (S. 2878, § 1801(a)); *id.* at 26,473, 27,208, 27,251-27,252 (H.R. 5484, § 1801); *id.* at 27,189 (Sen. Leahy) (explaining that the FOIA amendments' text was "identical" to that in S. 774 and that the Senate Report on S. 774 explained the "meaning and intended effect of the amendments"). Senator Hatch reiterated that the amendment to Exemption 7(F) would correct "an obvious and absurd limitation" in the existing law which does not extend "protection to the life of any natural person." *Id.* at 26,770. After a House amendment to the Senate's Exemption 7(F) proposal employed the phrase "any individual" rather than "any natural person," *id.* at 29,652, Senator Hatch clarified that the change in terminology did not effect any substantive change. See *id.* at 31,423-31,424 (revisions to Exemption 7 "derive precisely" from S. 774); see also *id.* at 29,619 (Rep. Kindness) (explaining that the Senate Report on S. 774 reflects the "meaning and intended effect of the [House] amendments"). Congress enacted H.R. 5484 into law. See Freedom of Information Reform Act of 1986, Pub. L. No. 99-570, Tit. I, Subtit. N, § 1802(a), 100 Stat. 3207-48 (amending Exemption 7(F)).

expected to endanger someone's life or physical safety.” *Id.* at 12 n.20, 18. That memoranda provides additional weight in favor of the government's construction of Exemption 7(F). See, e.g., *Abramson*, 456 U.S. at 622 n.5; *U.S. Dep't of State v. Washington Post Co.*, 456 U.S. 595, 602 n.3 (1982); *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 151 (1980).

The district court's atextual limitation on Exemption 7(F) does not follow from the legislative history cited by the court. The limitation does not relate to the motive of protecting people in the law enforcement sphere, such as victims, witnesses, informants, and families. See JA 52-53. And, although any additional limit on Exemption 7(F) could be viewed as limiting the 1986 amendment (see JA 53), nothing in the cited legislative history calls for the district court's particular limit. Indeed, under the district court's construction of Exemption 7(F), the 1986 amendment would have narrowed (not expanded) Exemption 7(F)'s protection in a critical respect. Before 1986, the requirement that disclosure would endanger “law enforcement personnel” did not require the government to identify particular at-risk officials. See, e.g., *LaRouche v. Webster*, No. 75-cv-6010, 1984 WL 1061, at *8 (S.D.N.Y. Oct. 23, 1984) (applying Exemption 7(F) to block public disclosure of an FBI report describing a home-made machine gun, in order to protect “law enforcement personnel” generally).

The district court also appears to have misunderstood the significance of the legislative history on which it relied. For example, the statement of the Deputy

Attorney General cited by the court explained that the language of Exemption 7 would be “modified slightly—not revised wholesale” and referred to two amendments unrelated to the language in dispute between the parties here. 131 Cong. Rec. 248 (1985) (discussing S. 774, 98th Cong., 1st Sess. (1983)). The Deputy Attorney General explained that amendments to FOIA should not “be evaluated by the simplistic measure of whether they provide for more or less disclosure,” but instead by whether they “bring about a better balance” between the competing values at stake. *Ibid.* She went on to express support for amending Exemption 7(F) to expand its protection from “law enforcement” to “the life of *any other person*.” *Id.* at 253. (emphasis added). The district court also relied on a floor statement by Representative English, but Representative English characterized the proposed amendments to Exemption 7(F) as “modest” and “slight” in the course of explaining that he “would not have chosen this time or this bill” to amend FOIA but that the changes “confirm[ed] [his] previously stated views” that the Department of Justice’s concerns “about the negative effects of the FOIA were greatly exaggerated.” 132 Cong. Rec. 29,616 (1986). After those remarks, Senator Hatch—the “principal author” and sponsor of the Exemption 7 amendments—emphasized that “[t]here should be no misunderstanding” that the relevant amendments “are intended to broaden the reach of this exemption” and “ease considerably [the government’s] burden in invoking it.” 132 Cong. Rec. 31,423-31,424 (1986).

3. In any event, even if the government were required to show a particularized threat to a discrete population to satisfy Exemption 7(F), the government made the requisite showing. In *PEER*, this Court declined to decide whether the Second Circuit had correctly interpreted “any individual” as used in Exemption 7(F) in its now-vacated decision in *ACLU v. Department of Defense*, which was the principal support relied on by the district court here. *PEER*, 740 F.3d at 206. This Court reasoned that, even under the standard articulated by the Second Circuit, the government would establish that Exemption 7(F) applied by showing that release of information could reasonably be expected to pose “a threat to the population living downstream of a dam.” *Ibid.* As this Court elaborated, “[t]errorists or criminals could use [the information in an inundation map for a dam] to determine whether attacking a dam would be worthwhile, which dam would provide the most attractive target, and what the likely effect of a dam break would be.” *Ibid.*

Similar analysis applies to SOP 303’s procedures for responding to crises such as terrorist attacks. Although the set of people who could be harmed as a result of disclosure of SOP 303 is large, there are identifiable groups who are more likely to be harmed. These include people near unexploded bombs, people who frequent high-value targets, and bomb squads and other first responders. Cf., e.g., *LaRouche*, 1984 WL 1061, at *8 (withholding FBI report describing a home-made machine gun, in order to protect “law enforcement personnel” generally); *Peter S. Herrick’s Customs & Int’l Trade Newsletter v. U.S. Customs & Border Prot.*, No. 04-377, 2006 WL 1826185, at

*8-*9 (D.D.C. June 30, 2006) (withholding portions of asset-seizure handbook because disclosure would risk danger to customs officials and “innocent third parties located in the vicinity of Customs’ officials, activities, or seized contraband”); *Los Angeles Times Commc’ns, LLC v. Dep’t of the Army*, 442 F. Supp. 2d 880, 898-900 (C.D. Cal. 2006) (withholding names of private security companies working in Iraq because of risk to unspecified “military personnel, [company] employees, and civilians”); *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1321-1322 (D. Utah 2003) (withholding agency maps showing areas subject to inundation from dam failures to protect individuals who could be at risk from terrorist-induced dam failures).

The fact that those procedures apply to all crises nationwide, and not simply to a single geographic region, should not alter that conclusion—just as Exemption 7(F) should apply not simply to an inundation map for a single dam but also to a map showing all inundation areas nationwide. Releasing procedures that apply to wireless networks nationwide runs a greater risk to a larger population of individuals. Congress could not have intended that only site-specific instructions could be withheld and that nationwide instructions must be released.

Accordingly, even under the rule applied by the district court, the judgment below should be reversed, and the Court should direct the entry of summary judgment in favor of the government. At a minimum, however, the agency should be permitted to elaborate on the factual points in its declaration in light of the district

court's adoption of a heightened standard for showing harm to a specifically identified individual or group of individuals.

B. The Department of Homeland Security Properly Withheld SOP 303 Under FOIA Exemption 7(E).

Because release of SOP 303 “could reasonably be expected to endanger the life or physical safety of any individual,” 5 U.S.C. § 552(b)(7)(F), it is not necessary for the Court to address whether it is also exempt under FOIA Exemption 7(E). Were the Court to reach that issue, however, DHS also properly withheld SOP 303 pursuant to Exemption 7(E).

1. Exemption 7(E) protects “records or information compiled for law enforcement purposes” that “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law,” 5 U.S.C. § 552(b)(7)(E).

a. Before 1986, Exemption 7 applied to “*investigatory* records compiled for law enforcement purposes,” and Exemption 7(E) added a further requirement that production would also “disclose *investigative* techniques and procedures.” 5 U.S.C. § 552(b)(7)(E) (1982) (emphases added). This text gave rise to two distinct requirements: (1) the threshold Exemption 7 requirement for “investigatory” records being compiled for law enforcement purposes and (2) the Exemption 7(E) requirement that production would disclose “investigative” procedures or techniques.

The first requirement (Exemption 7's threshold requirement) concerned compilation of the agency "records" themselves, and confined the scope of Exemption 7 to only "investigatory records" compiled for certain purposes. The second requirement (Exemption 7(E)'s additional requirement) focused on a specific type of "techniques and procedures"— "*investigative* techniques and procedures" — identified within such records, and limited Exemption 7(E) only to contexts where production of the records would disclose such "investigative techniques and procedures." The use of the word "investigative" in Exemption 7(E) as an adjective that modified the term "techniques and procedures" made clear that the specific "techniques and procedures" must themselves have been "investigative" in nature.

Courts concluded that this text imposed two distinct requirements. First, as a threshold matter, Exemption 7 applied only to records "compiled in the course of a *specific* investigation," *i.e.*, "an investigation directed at specific persons." *E.g.*, *Sladek v. Bensinger*, 605 F.2d 899, 903 (5th Cir. 1979) (emphasis added). Second, Exemption 7(E) applied only if, in addition, disclosure would reveal particular type of techniques and procedures: "*investigative* techniques and procedures." *E.g.*, *ibid.* (emphasis added); see, *e.g.*, *Shaver v. Bell*, 433 F. Supp. 438, 441 (N.D. Ga. 1977) (giving as an example of an "investigative technique" the "the use of bait money as a means of effecting a successful investigation of criminal offenses"). Thus, Exemption 7(E)'s pre-1986 text was understood to apply to "only [1] records compiled in the course of an

investigation directed at specific persons are exempt and then only if [2] disclosure would reveal investigative techniques and procedures.” *Sladek*, 605 F.2d at 903.

b. In 1986, Congress amended Exemption 7’s threshold requirement and Exemption 7(E)’s additional investigative requirement. First, Congress deleted the word “investigatory” from Exemption 7’s prefatory text and broadened the exemption to apply to “records and information” compiled for law enforcement purposes. This change was “intended to ensure that sensitive law enforcement information is protected under Exemption 7 regardless of the particular format or record in which the record is maintained.” Senate Report 23. Senate Report No. 98-221 illustrated the problem that the amendment was designed to address by citing *Sladek* with a parenthetical showing that *Sladek* had denied Exemption 7 protection to a DEA agents manual because the manual “was not compiled in the course of a specific investigation.” *Ibid.*⁵

Second, Congress deleted the word “investigative” from Exemption 7(E) and, at the same time, modified the remaining text (“techniques and procedures”) by adding the phrase “for law enforcement investigations or prosecutions.” This change eliminated the requirement that covered techniques and procedures must themselves be “investigative” in nature. In other words, Exemption 7(E) now covers *non-*

⁵ This Court has found it “clear” that Exemption 7’s “amended threshold” text now allows withholding “even when the materials have not been compiled in the course of a specific investigation.” *Tax Analysts v. IRS*, 294 F.3d 71, 79 (D.C. Cir. 2002).

investigative techniques or procedures, so long as they are “for law enforcement investigations or prosecutions.” 5 U.S.C. § 552(b)(7)(E). That statutory text indicates that Congress understood that law enforcement investigations can involve both investigatory and non-investigatory elements and that Congress intended to protect all such “procedures,” even if they are for the non-investigatory parts of law enforcement investigations, so long as the procedures are for use in such investigations. The legislative history thus confirms that the textual change was “intended to make clear that ‘techniques and procedures for law enforcement investigations and prosecutions’ can be protected, regardless of whether they are ‘investigative’ or non-investigative.” Senate Report 24.

The Attorney General’s Memorandum on the 1986 FOIA Amendments likewise concluded that the amendment to Exemption 7(E) “should considerably expand the breadth of Exemption 7(E) protection” to “encompass[] *all* ‘techniques and procedures for law enforcement investigations or prosecutions.’” *Attorney General’s Memorandum* 15 (emphasis added). The Attorney General explained that the revised Exemption 7(E) “authorizes the withholding of information consisting of, or reflecting, a law enforcement ‘technique’ or a law enforcement ‘procedure,’ . . . [b]ut such items no longer are required to be ‘investigatory’ or ‘investigative’ in character in order to be withheld.” *Ibid.* “Rather, a technique or procedure now can properly be protected under Exemption 7(E) wherever it is ‘for law enforcement investigations or prosecutions’ *generally*.” *Ibid.* (emphases added).

c. SOP 303 easily meets this requirement. SOP 303 contains procedures that apply only when there is a serious threat, which undoubtedly will trigger a law enforcement investigation. Choosing whether, when, and where to shut down a cellular network is a logical component of an ongoing investigation triggered by the threat. As such, the procedures in SOP 303 are procedures “*for* law enforcement investigations,” 5 U.S.C. § 552(b)(7)(E) (emphasis added), even if the procedures may not themselves be deemed “investigative” in nature. See Senate Report 24 (procedures themselves need not be “investigative” to be covered by Exemption 7(E)).

Moreover, the procedures in SOP 303 themselves serve an investigative function because of their role in the accompanying investigations into where unexploded bombs are located, who is responsible, and where the suspects can be found. SOP 303 includes techniques and procedures for “preventing and/or mitigating explosions” and for minimizing interference with “first-responders” and “the public[’s] use [of] wireless phones for calls, including 911 calls.” JA 18. Procedures for stopping detonation of bombs, in addition to saving the lives of bystanders, also protect first responders investigating the events, witnesses who can offer helpful clues, and valuable physical evidence such as undetonated bombs. Procedures for ensuring that first responders such as police bomb squads and arson units can quickly and effectively deploy, and that the public can make calls, including 911 calls, are tied directly to law enforcement investigations. As such, the procedures

in SOP 303 are procedures “*for* law enforcement investigations,” 5 U.S.C.

§ 552(b)(7)(E) (emphasis added).

2. The district court erred in reasoning that because an “ordinary speaker” would not “describe SOP 303 . . . as an evidence-gathering technique,” Exemption 7(E) is therefore inapplicable. JA 50.

The court erred by requiring that disclosure would reveal an “evidence-gathering technique,” *i.e.*, an investigative procedure or technique, rather than a procedure or technique “*for* law enforcement investigations,” 5 U.S.C. § 552(b)(7)(E) (emphasis added). In other words, the court mistakenly applied the pre-1986 requirement that production would disclose “disclose *investigative* techniques and procedures,” 5 U.S.C. § 552(b)(7)(E) (1982) (emphasis added), rather than the present requirement that production would disclose “techniques and procedures *for* law enforcement investigations,” 5 U.S.C. § 552(b)(7)(E) (emphasis added). As we have discussed, the 1986 textual changes made clear that the “techniques and procedures” referred to in Exemption 7(E) no longer need to be investigative in nature. The deletion of the word “investigative” and the new textual requirement that the “techniques and procedures” must be “*for* law enforcement investigations” demonstrates that Congress understood that such “investigations” have both investigative and non-investigative elements and that Exemption 7(E) was designed to protect the “techniques and procedures” for both elements of investigations. See Senate Report 24 (Exemption 7(E) “make[s] clear that ‘techniques and procedures for

law enforcement investigations and prosecutions’ can be protected, regardless of whether they are ‘investigative’ or non-investigative”).

Moreover, even if the procedures must themselves be investigative (which they do not), the court erred by asking only how an “ordinary speaker” would “describe SOP 303” and by assuming that a technique or procedure may serve only one function. Producing SOP 303 would not just disclose a procedure for saving lives; it would also disclose a procedure for safely deploying first responders, for preserving evidence, and for minimizing disruption to 911 calls. Cf. *PEER*, 740 F.3d at 204-205 (Exemption 7(E) covers “emergency action plans [that] contain guidelines that inform emergency personnel how to manage a dam failure,” including “security precautions . . . during emergency conditions,” and “surveillance and detection of the cause of an emergency dam failure”). The district court’s contrary conclusion was in error.

CONCLUSION

The judgment of the district court should be reversed.

Respectfully submitted,

STUART F. DELERY

Assistant Attorney General

RONALD C. MACHEN, JR.

United States Attorney

SHARON SWINGLE

/s/ Adam Jed

ADAM C. JED

(202) 514-8280

Attorneys, Appellate Staff

Civil Division, Room 7240

U.S. Department of Justice

950 Pennsylvania Ave., N.W.

Washington, DC 20530

JUNE 2014

**CERTIFICATE OF COMPLIANCE WITH
FEDERAL RULE OF APPELLATE PROCEDURE 32(a)**

I hereby certify that this brief complies with the requirements of Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in 14-point Garamond, a proportionally spaced font. I further certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 6,470 words, excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii), according to the count of Microsoft Word.

/s/ Adam Jed

Adam C. Jed

CERTIFICATE OF SERVICE

I hereby certify that on June 4, 2014, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system.

/s/ Adam Jed

Adam C. Jed

ADDENDUM

5 U.S.C. § 552 (excerpts)

(a) Each agency shall make available to the public information as follows:

* * *

(b) This section does not apply to matters that are—

* * *

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information

(A) could reasonably be expected to interfere with enforcement proceedings,

(B) would deprive a person of a right to a fair trial or an impartial adjudication,

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual;

* * *